UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

COREY HEARD, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	
	)	**No. 19 C 4158**
v.	)	
	)	**Chief Judge Rebecca R. Pallmeyer**
BECTON, DICKINSON & CO.,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Corey Heard filed this proposed class action against Becton, Dickinson & Co. ("BD"), the manufacturer of an automated medication dispensing system that requires users to scan their fingerprints. Mr. Heard alleges that BD violated and continues to violate several provisions of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq*. The case was filed in state court, but BD removed on the basis of diversity jurisdiction and the Class Action Fairness Act. 28 U.S.C. §§ 1332(d), 1453. In an earlier ruling, *see Heard v. Becton, Dickinson & Co*., 440 F. Supp. 3d 960 (N.D. Ill. 2020) ("*Heard I*"), the court dismissed Plaintiff's complaint but gave him leave to amend, and Plaintiff has done so. BD again moves to dismiss, and has moved to strike the class allegations in Plaintiff's amended complaint. For the reasons set forth below, the motion to dismiss [43] is denied, and the motion to strike [45] is denied without prejudice.

BACKGROUND

At this stage of the proceedings, the court accepts the allegations in the First Amended Complaint ("FAC") as true. BD manufactures medical technology and devices for healthcare institutions, including dozens of hospitals in Illinois. (FAC [37] ¶ 1.) One of its products, the Pyxis MedStation system ("Pyxis"), is an automated medication dispensing system; the system requires that, in order for hospital workers to obtain medication for distribution to patients, the workers

must submit to a fingerprint scan.[1] (*Id.*) The purpose of this technology is to improve hospitals' ability to control access to medication. (*Id.* ¶ 54.) Hospital workers first enroll in the Pyxis system by placing a finger on a "platen," a flat plate on the Pyxis device's fingerprint scanner, and the device captures an image of the fingerprint. (*Id.* ¶ 6.) The device then extracts unique features in the fingerprint to create a user template, which is stored both on the device and in a database. (*Id.*) Once users have enrolled their fingerprints, the device can verify or identify a user's fingerprint, depending on the device's configuration.[2] (*Id.* ¶ 4.) In a hospital setting, users can access multiple Pyxis devices within the hospital because Pyxis software allows the devices to communicate with one another. (*Id.* ¶¶ 2–3.) Pyxis devices also share the unique user templates and data from subsequent fingerprint scans with BD's servers. (*Id.* ¶¶ 7, 9.)

Corey Heard ("Plaintiff") is an Illinois resident who works as a respiratory specialist. (*Id.* ¶¶ 27, 61.) Since 2015, he has worked for five hospitals that use Pyxis devices.[3] (*Id.* ¶ 61.) As a condition of his employment, Plaintiff was required to enroll his fingerprint with the devices and to scan his fingerprint each time he accessed a device. (*Id.* ¶¶ 62, 67.) Plaintiff re-enrolled with Pyxis devices each time he began new employment with a hospital. (*Id.* ¶ 63.) Plaintiff alleges not only that the hospitals stored his fingerprint data, but also that each time he accessed a Pyxis

---

[1] BD disputes that its Pyxis devices scan users' "fingerprints" within the meaning of BIPA. (Def.'s Mem. in Support of Mot. to Dismiss [44] (hereinafter "MTD Mem.") at 2 n.2 (citing 740 ILCS 14/10).) The court understands BD to suggest that the devices extract certain information from a fingerprint, but do not collect or store a copy of the fingerprint itself. BD is welcome to raise this argument again after discovery.

[2] As the court understands the FAC, "verification" compares the input fingerprint against all of the fingerprints enrolled on the device to find a matching set of *prints*, whereas "identification" compares the input fingerprint against all fingerprints enrolled on the device to find a matching *user*. (*Id.* ¶ 5.)

[3] As this court previously noted, *Heard I*, 440 F. Supp. 3d at 963 n.1, Mr. Heard is the lead plaintiff in at least four other putative class actions raising BIPA claims in state court. *Heard v. Omnicell*, No. 2019-CH-06817 (Ill. Cir. Ct. Cook Cnty.); *Heard v. Weiss Mem'l Hosp.*, No. 2019-CH-06763 (Ill. Cir. Ct Cook Cnty.); *Heard v. St. Bernard Hosp.*, No. 2017-CH-16828 (Ill. Cir. Ct. Cook Cnty.); *Heard v. TCH-North Shore, Inc.*, No. 2017-CH-16918 (Ill. Cir. Ct. Cook Cnty.).

device, BD collected his fingerprint data and stored it on its servers. (*Id*. ¶¶ 65–68.) Plaintiff alleges that he has never been informed of: (1) the purposes or length of time for which Defendant has collected, stored, and/or disseminated his biometric data; (2) whether BD has a biometric data retention policy; or 3) whether BD will ever permanently delete his data. (*Id*. ¶ 69–70.) Furthermore, he has never been presented with or signed a written release allowing BD to collect, store, or disseminate his biometric data. (*Id*. ¶ 71.) Plaintiff seeks certification of the following class: "All users in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by Defendant during the applicable statutory period." (*Id*. ¶ 83.)

Enacted in 2008, the BIPA protects Illinois residents' privacy interests in their biometric information. The Illinois General Assembly found that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). The Act defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. In turn, "biometric identifier" means "a retina or iris scan, *fingerprint*, voiceprint, or scan of hand or face geometry." *Id*. (emphasis added). By its nature, biometric information cannot be changed: "once compromised, the individual has no recourse [and] is at heightened risk for identity theft." *See* 740 ILCS 14/5(c). Section 15 of the Act regulates the collection, retention, disclosure, and dissemination of biometric information and biometric identifiers (collectively referred to in this opinion as "biometric data") by private entities. Among other things, Section 15 requires that private entities establish a retention schedule and guidelines for permanently destroying biometric data when the purpose for collecting it is satisfied, or within three years of the individual's last interaction with the private entity. 740 ILCS 14/15(a). The Act defines "private entity" broadly to include "any individual, partnership, corporation, limited liability company, association, or other

group, however organized," subject to exceptions not relevant here.[4] 740 ILCS 14/10. Section 20 provides a private right of action for persons aggrieved by a violation of the Act, who may receive statutory damages, attorneys' fees, and injunctive relief.

Plaintiff brings three claims against BD on behalf of himself and the putative class. Count I alleges a violation of Section 15(a) for "failure to institute, maintain and adhere to [a] publicly-available retention schedule." (*Id*. ¶¶ 93–101.) Specifically, Plaintiff alleges that BD lacks retention schedules and guidelines for the destruction of biometric data and has failed to destroy that data when the purpose for it has been satisfied or within three years of Plaintiff's contact with BD. (FAC ¶ 100.) This failure to destroy the biometric data of Plaintiff and others similarly situated creates a "material risk" that third parties will unlawfully access their biometric data. (*Id*. ¶ 23.) Count II alleges a violation of Section 15(b) for "failure to obtain informed written consent and release before obtaining biometric identifiers or information." (*Id*. ¶¶ 102–111.) Finally, Count III alleges a violation of Section 15(d) for "disclosure of biometric identifiers and information before obtaining consent." (*Id*. ¶¶ 112–120.) The recipients of this data are "currently unknown," but include "third parties that host biometric data in their data center(s)." (*Id*. ¶ 18.) Plaintiff seeks a declaratory judgment that BD's conduct violated the BIPA, injunctive relief, statutory damages, and attorneys' fees. (*Id*. ¶¶ 101, 111, 120.)

DISCUSSION

I. Motion to Dismiss for Failure to State a Claim

In order to survive a motion to dismiss under FED. R. CIV. P. 12(b)(6), a complaint must contain "enough factual matter (taken as true)" to suggest that a plaintiff is entitled to relief. *Bell*

[4] Plaintiff has alleged that BD, a New Jersey corporation registered to do business in Illinois, is a private entity within the meaning of BIPA. (FAC ¶¶ 28, 96, 105, 115.) Defendant does not dispute that it is a private entity under BIPA; instead, BD contends that it is exempt because it is not Plaintiff's employer or, alternatively, it is protected from liability by a so-called "health care exemption." (*See* MTD Mem. at 6–7, 9–11.) The court addresses these arguments below.

Atl. Corp. v. Twombly, 550 U.S. 544, 556 (2007). Courts generally "do not require heightened fact pleading of specifics, but only enough facts to state a claim to relief that is plausible on its face." *Id*. at 570. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). In other words, "the plaintiff must give enough details about the subject-matter of the case to present a story that holds together." *Swanson v. Citibank, N.A.*, 614 F.3d 400, 404 (7th Cir. 2010). As this court emphasized in its previous memorandum opinion, complaints cannot "merely parrot the statutory language of the claims that they are pleading"; rather, they must provide "some specific facts to ground those legal claims." *Heard I*, 440 F. Supp. 3d at 966 (citing *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir. 2009)).

BD argues that Plaintiff has once again failed to state a claim under Sections 15(a), 15(b), and 15(d) of the BIPA. Alternatively, BD contends that Plaintiff's FAC must be dismissed because of BIPA's purported health care exemption. Finally, BD suggests that the complaint is deficient for failure to plead negligence, recklessness, or intent. The court begins by addressing the adequacy of Plaintiff's allegations before turning to Defendant's alternative arguments.

A. Section 15(a)

Section 15(a) of the BIPA requires private entities "in possession" of biometric data to "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." As this court previously observed, the BIPA does not define what it means to be "in possession of" biometric data. *Heard I*, 440 F. Supp.3d at 968.

1. Standing

Article III standing is a prerequisite to the exercise of federal courts' jurisdiction. *See* U.S. Const. art. III, § 2; *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). Typically, a plaintiff bears the burden of establishing standing, but where, as here, a case has been removed to federal court, the burden is on the defendant. *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 620 (7th Cir. 2020). To establish standing, "[t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo*, 136 S. Ct. at 1547. In *Bryant*, the Seventh Circuit held that a plaintiff lacked Article III standing to bring a claim under Section 15(a) for failure to *publicly disclose* a retention policy and schedule for the destruction of biometric data. 958 F.3d at 626. The plaintiff had not alleged a "concrete and particularized injury" from defendant's statutory violation because "the duty to disclose under section 15(a) is owed to the public generally, not to particular persons whose biometric information the entity collects." *Id*. The court cautioned that its holding was narrow, and it reserved the question of standing requirements for claims under other portions of Section 15(a). *Id*.

In a footnote, Plaintiff asks that the court sever and remand his Section 15(a) claim to state court for lack of standing. (Pl.'s Opp'n to Def.'s Mot. to Dismiss [53] (hereinafter "Opp'n to MTD") at 11 n.2 (citing *Bryant*).) Although Plaintiff does not specify which element of Article III standing he believes is lacking, the court presumes that Plaintiff believes his allegations are akin to those in *Bryant* with respect to injury in fact. *See Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1151 (7th Cir. 2020) (observing that "[t]he injury-in-fact requirement is usually the main event in litigation over standing"). Defendant objects and requests that if the court considers remanding Plaintiff's Section 15(a) claim, BD be given an opportunity for additional briefing. (Def.'s Reply in Support of Mot. to Dismiss [57] (hereinafter "Def.'s MTD Reply") at 5 n.4.) Meanwhile, the Seventh Circuit has clarified that some plaintiffs may have standing for claims

under Section 15(a). *See Fox*, 980 F.3d at 1155–56. Because the court concludes that the allegations of the FAC are sufficient to establish standing, the court declines to order remand.

In *Fox*, the Seventh Circuit held that a plaintiff had standing to bring a Section 15(a) claim alleging that a defendant failed to "develop, publicly disclose, *and comply with* data retention and destruction policies." *Id*. at 1149 (emphasis in original). This made her Section 15(a) claim "much broader than Bryant's." *Id*. at 1154. The court emphasized the importance of a plaintiff's factual allegations to show a concrete and particularized injury arising from a violation of Section 15(a). Specifically, Fox alleged that her former employer had unlawfully retained her biometric data after she left. *Id*. at 1150. The court observed that "an unlawful *retention* of a person's biometric data is as concrete and particularized an injury as an unlawful *collection* of a person's biometric data" in violation of Section 15(b). *Id*. at 1155 (emphasis in original). The Court of Appeals concluded that plaintiff had standing, and reversed the district court's remand order. *Id*. at 1156.

Here, Mr. Heard has likewise alleged not only that BD failed to make a retention schedule and destruction policy publicly available, but also that BD did not adhere to such a policy by deleting biometric data. (*See* FAC ¶¶ 94–95.) Plaintiff further alleges that BD "has not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied." (*Id*. ¶ 100.) District courts interpreting *Fox* have concluded that plaintiffs making similar allegations have standing under Section 15(a). *See Roberson v. Maestro Consulting Servs. LLC*, ___ F. Supp. 3d ___, No. 20-CV-00895-NJR, 2020 WL 7342693, at *4 (S.D. Ill. Dec. 14, 2020) (plaintiffs had standing to bring two Section 15(a) claims against their employer where first claim alleged "failure to properly establish publicly-available policy" and second claim alleged "failure to comply with established retention schedule and destruction guidelines"); *Marsh v. CSL Plasma Inc.*, ___ F. Supp. 3d ___, No. 19 C 6700, 2020 WL 7027720, at *4 (N.D. Ill. Nov. 30, 2020) (finding standing under Section 15(a) where plaintiffs alleged that defendant failed to comply with BIPA's requirement that collectors of

biometric data develop a retention policy); *Neals v. ParTech, Inc.*, No. 19-CV-05660, 2021 WL 463100, at *4–5 (N.D. Ill. Feb. 9, 2021) (same).[5] Because the court concludes that Mr. Heard has alleged a "concrete and particularized injury" from BD's failure to delete his biometric data, the court denies his request to remand and turns to the sufficiency of his Section 15(a) claim.

2. Sufficiency

The court previously held that Plaintiff failed to state a claim under Section 15(a) because he had not adequately pleaded that BD had "possession" of his biometric data. *Heard I*, 440 F. Supp. 3d at 968. Applying the ordinary meaning of "possession" under Illinois law, the court concluded that Plaintiff's original complaint did not allege that BD "exercised any form of control over the data or. . . held the data 'at [its] disposal.'" (*Id*. (citing *People v. Ward*, 215 Ill. 2d 317, 325, 830 N.E.2d 556, 560 (2005)). In response, Plaintiff has added several allegations that, while subtle, push this claim "across the line from conceivable to plausible." *Twombly*, 550 U.S. at 557. The FAC clarifies that when a user enrolls in a Pyxis system, BD stores users' fingerprints on *both* the Pyxis devices and BD's servers. (*See* FAC ¶¶ 6–9, 46, 48–50, 65, 68; Opp'n to MTD at 9–10.) The FAC also notes that BD markets its devices as offering an "integrated medication management platform, through which Becton provides a single, centralized location for hospitals to manage data, along with dedicated support services through which Becton can access the biometric data collected." (FAC ¶ 8.) In other words, the Pyxis system is not hermetically sealed within a hospital; users' biometric data flows back to BD's servers (and potentially third-party data

[5] The court notes that the defendants in these three cases had different relationships with the plaintiffs that could affect plaintiffs' ability to succeed on the merits. In *Roberson*, the defendants (a network of various nursing homes) required employees to scan their fingerprints or handprints for time and attendance. *Roberson*, 2020 WL 7342693, at *1. In *Marsh*, plasma donors sued a plasma-donation company that required donors to scan their fingerprints. *Marsh*, 2020 WL 7027720, at *1. Finally, in *Neals*, a restaurant required its employees to scan their fingerprints for time and attendance. Rather than suing her employer, the plaintiff sued the developer of the fingerprint-scanning system. *Neals*, 2021 WL 463100, at *1. Of the three, *Neals* is the most analogous to this case because the defendant is a third party outside of the employment relationship.

centers, as discussed below) for analysis and support services. These allegations satisfy the court that BD was plausibly "in possession" of users' biometric data.

Defendant responds that the FAC is nevertheless insufficient because "Plaintiff still makes no allegation that BD could freely access biometric data, that BD exercised any control over the data, or even how BD received it." (Def.'s Mem. in Support of Mot. to Dismiss [44] (hereinafter "MTD Mem.") at 8.) These arguments are unpersuasive. At this stage, Plaintiff need not show in granular detail the precise means by which users' biometric data travelled from Pyxis devices to BD's servers (i.e., via ethernet cable or Wi-Fi). Plaintiff's allegation that BD provides support services by analyzing data collected from Pyxis devices is enough to suggest that BD exercises some form of control over users' biometric data and therefore is in possession of the data.

B. Section 15(b)

Section 15(b) of BIPA prohibits private entities from "collect[ing], captur[ing], purchas[ing], receiv[ing] through trade, or otherwise obtain[ing] a person's or a customer's biometric identifier or biometric information" without their informed consent. 740 ILCS 14/15(b). To obtain consent, an entity must inform the subject in writing that her data is being collected or stored; specify the purpose and length of time for which the data is being collected, stored, and used; and receive a written release. 740 ILCS 14/15(b)(1)–(3). The FAC, like the original complaint, alleges that BD has not obtained informed consent from Pyxis users. (FAC ¶¶ 16–17, 51–52, 69, 71, 108–110.) The question here is whether the FAC, unlike the original complaint, sufficiently alleges that BD "collect[ed], capture[d], . . . or otherwise obtain[ed]" biometric data. 740 ILCS 14/15(b). The court concludes that it does.

This court previously concluded that mere possession of biometric data is insufficient to trigger Section 15(b)'s requirements. *Heard I*, 440 F. Supp.3d at 965 (citing *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 285–86 (N.D. Ill. 2019); *Bernal v. ADP,* LLC, No. 2017-CH-12364, 2019 WL 5028609, at *1 (Ill. Cir. Ct. Cook Cnty. Aug. 23, 2019)). Instead, "an entity must,

at a minimum, take an active step" to collect or otherwise obtain biometric data. *Heard I*, 440 F. Supp. 3d at 966. The court concluded that Plaintiff's original complaint failed to allege an "affirmative act" by which BD collected the data. *Id*. at 966–67. As another district court has explained, however, Section 15(b) applies prospectively to the collection of biometric data after the date of BIPA's enactment, while other sections of the Act are aimed at defendants who had collected data before BIPA was adopted and remained in possession of that data. *Figueroa v. Kronos*, 454 F. Supp. 3d 772, 783–84 (N. D. Ill. 2020) (Feinerman, J.). The fingerprint scans at issue in this case were collected after the enactment of BIPA, and BD is in possession of that data because it remains stored on BD's servers, so it is fair to conclude that BD collected or otherwise obtained the data for purposes of Section 15(b).

In any event, the court now concludes that the FAC has sufficiently alleged an active step by BD to collect, capture, or otherwise obtain Pyxis users' biometric data. 740 ILCS 14/15(b). As discussed above, the FAC alleges that when a user enrolls in the Pyxis system, the device scans the user's fingerprint, extracts the unique features of that fingerprint to create a user template, and then stores users' biometric information both on the device *and* in BD's servers. (*See* FAC ¶¶ 6–9, 46, 48–50, 65.) Data from subsequent scans are also stored on BD's servers. (*See id*. ¶ 68.) These allegations suggest that BD itself plays an active role in collecting or otherwise obtaining users' biometric information from the Pyxis devices. *See Figueroa*, 454 F. Supp. 3d at 784 ("The complaint alleges that [the defendant] 'stored,' 'used,' and 'disclosed' Plaintiffs' biometric data . . . and to have done those things Kronos necessarily first had to 'obtain' the data.").

BD argues that Plaintiff's own allegations suggest that it is the hospitals, not BD, that store users' biometric information on their own systems and servers. (MTD Mem. at 4–5.) BD may ultimately prevail on this point, particularly given that users like Plaintiff need to enroll with a Pyxis device each time they begin working at a new hospital. (*See* FAC ¶ 63.) The court agrees with

Plaintiff, however, that he is not required to prove the merits of his claims at the pleading stage. (*See* Opp'n to MTD at 6.) It is entirely plausible that users' biometric information is stored on *both* the hospitals' servers and BD's servers.[6]

Alternatively, Defendant argues that Section 15(b) does not apply to third-party vendors, like BD, when the collection of biometric data occurs in the context of an employment relationship. (*See* MTD Mem. at 6–7.) In such situations, BD asserts, the employer—not the vendor—should obtain consent from an employee. (MTD Reply at 3–5.) The court declined to address this argument in its prior opinion, *see Heard I*, 440 F. Supp. 3d at 968, and rejects that argument now for the following reasons. First, by its language, BIPA reaches a wide range of "private entit[ies]." 740 ILCS 14/10 (defining "private entity" as "any individual, partnership, corporation, limited liability company, association, or other group, however organized"). BD points to BIPA's definition of "written release" to argue that vendors are not required under Section 15(b) to obtain consent from their customers' employees. (*See* MTD Mem. at 6 (quoting 740 ILCS 14/10 ("'written release' means . . . in the context of employment, a release executed by an employee as a condition of employment").) But that definition does not foreclose the possibility of liability under other provisions of Section 15(b). Recall that Section 15(b) requires not only that private entities receive a written release, *see* 740 ILCS 14/15(b)(3), but also that they inform the subject in writing that their biometric data is being collected or stored and the specific purpose and length of time for which that is happening. *See* 740 ILCS 14/15(b)(1)–(2). Accordingly, even if BD is not required

[6] In a footnote, BD argues that Plaintiff should be judicially estopped from arguing that his biometric data is stored on BD's servers because he has argued in another BIPA suit—against his former employer—that the hospital stored his biometric data. (MTD Reply at 2 & n.2 (citing Compl., *Heard v. Weiss Mem'l Hosp.*, No. 19 CH 06763, Ex. A to MTD Mem. [44-1] ¶¶ 5, 51–52).) The court need not wade into the doctrine of judicial estoppel because, as noted above, it is entirely plausible that his biometric data is stored on both the hospital's servers and BD's servers. Thus, Plaintiff's arguments in this suit do not necessarily contradict his factual positions in other suits.

to obtain a written release from end users, it is still subject to Section 15(b)(1) and (2). *See Figueroa*, 454 F. Supp. 3d at 783.

Notably, at least one district court has held that third-party vendors like BD are subject to Section 15(b)(3) as well. In *Figueroa v. Kronos*, two employees sued the manufacturer of biometric-based time clocks for various BIPA violations, even though their employers had required them to use the equipment as a condition of employment. 454 F. Supp. 3d at 779. The court held that the employees had stated a claim under Section 15(b) and rejected the manufacturer's argument that time clock vendors owe no Section 15(b) duties to their customers' employees. See *Figueroa*, 454 F. Supp. 3d at 783–85 ("Even if Kronos's obtaining Plaintiffs' data occurred 'in the context of employment'—as opposed to in the context of a business-to-business relationship between Kronos and [Plaintiffs'] employers—Kronos still was a 'private entity' that 'collect[ed]' or 'obtain[ed]' Plaintiffs' data, and thus remained obligated to receive a release from them as a condition of their employment."). This interpretation of BIPA is hardly, as BD argues, an "absurd result" that would justify disregarding the statute's plain meaning. (MTD Mem. at 7 (citing *People v. Hanna*, 800 N.E. 2d 1201, 1208–09, 207 Ill.2d 486, 499–500 (Ill. 2003)).)

BD has identified two state court cases that reached the opposite conclusion: *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *1 (Ill. Cir. Ct. Cook Cnty. Aug. 23, 2019) and *Cameron v. Polar Tech Indus.*, No. 2019 CH 000013 (Ill. Cir. Ct. DeKalb Cnty. Aug. 23, 2019). (*See* Ex. 1 to MTD Reply [57-1].) Both cases involved employees who sued a biometric timeclock vendor that provided devices that their employers required them to use. Yet these courts' discussion of Section 15(b) is cursory and ultimately unpersuasive. The *Bernal* court's decision rested not on the inapplicability of Section 15(b) to third-party vendors, but on the insufficiency of the plaintiff's complaint on that count. *Bernal*, 2019 WL 5028609, at *2. And the *Cameron* court acknowledged that at the time of its decision, there was no case interpreting "written release" as the defendants had proposed. *Cameron*, No. 2019 CH 000013, at *32–34. Since then, two district

courts have rejected defendants' attempts to extend those cases. *See Figueroa*, 454 F. Supp. 3d at 784–85; *Neals v. PAR Tech Corp.*, 419 F. Supp. 3d 1088, 1092 (N.D. Ill. 2019) ("To the extent those decisions stand for the proposition that the BIPA exempts a third-party non-employer collector of biometric information when an action arises in the employment context, the Court disagrees with those decisions because there is no textual support whatsoever for such a restricted view of the statute's application."). The court agrees with the *Figueroa* court's interpretation of the statute and rejects Defendant's argument that it should be exempt from liability under Section 15(b) on this theory.

C. Section 15(d)

Section 15(d) of BIPA provides that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information" without consent. 740 ILCS 14/15(d). This court previously concluded that Plaintiff failed to state a claim under this provision because he had not alleged that BD was in possession of his biometric data, and because he "offer[ed] no basis for the allegation that BD disclosed his biometric data." *Heard I*, 440 F. Supp. 3d at 969. As discussed above regarding Plaintiff's Section 15(a) claim, the FAC now sufficiently alleges possession. The remaining issue is whether the FAC sufficiently alleges disclosure to third parties. The court concludes that it does and denies Defendant's motion to dismiss this claim.

Unlike Plaintiff's original complaint, the FAC does not allege disclosure "upon information and belief." (*See* Opp'n to MTD at 11.) Rather, Plaintiff affirmatively alleges that BD disseminates biometric data to third-party data centers. (*See* FAC ¶¶ 18, 77.) Plaintiff concedes that the identities of these third parties are "currently unknown," but insists that "[t]he very nature of Defendant's violations of Section 15(d)—failing to gain informed consent of dissemination of users' biometric data—makes it impossible to know *exactly* to whom Plaintiff's and other users' biometric data was disseminated." (Opp'n to MTD at 11 (emphasis in original).) Defendant

responds that the FAC still does nothing more than "parrot the statutory language" and is based on pure speculation. (MTD Mem. at 9 (quoting *Brooks*, 578 F.3d at 581).) Defendant is correct that Plaintiff's allegations regarding disclosure are still quite thin (*see* FAC ¶¶ 18, 77), but the court concludes that, when combined with his allegations that BD stores biometric data collected from the Pyxis devices on its own servers, it is at least plausible that those servers are backed up in third-party data centers. (*See id*. at ¶¶ 6–9, 46, 48–50, 65, 68.) In turn, because BD does not inform users of its Pyxis devices "to whom the data is disclosed," much less obtain their consent to do so, Plaintiff has stated a claim for Section 15(d).

D. Health Care Exemption

In the alternative, BD urges that Plaintiff's claims be dismissed on the basis of a purported "health care exemption" to the reach of BIPA. (MTD Mem. at 9.) BD locates this "exemption" in the BIPA's definition of "biometric identifiers," which excludes (1) "information captured from a patient in a health care setting or [(2)] information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act [(HIPAA)] of 1996." 740 ILCS 14/10. The first clause of this sentence ("information captured from a patient in a health care setting") plainly applies to *patients*, not health care workers like Mr. Heard. The closer question is whether the second clause ("information collected, used, or stored for health care treatment, payment, or operations under [HIPAA]") applies to health care workers' biometric information. BD argues that it does, insisting that the second clause "must be read to reach information other than that collected from a patient so as to avoid rendering it superfluous." (MTD Mem. at 10 (emphasis omitted).) Pyxis users, like Mr. Heard, scan their fingerprints in order to access medication that they will then administer to patients, so users' biometric information is arguably "collected, used or stored *for health care treatment*." 740 ILCS 14/10 (emphasis added). Plaintiff disagrees, arguing that the statute is

more sensibly read as excluding the biometric information of patients, not health care workers or providers, from protection under BIPA. (Opp'n to MTD at 11–15.)

The court previously declined to assess this argument because Mr. Heard's initial complaint failed to state a claim. *Heard I*, 440 F. Supp. 3d at 965. At the time, the court agreed with the observation in *Bruhn v. New Albertson's*: it seemed unlikely that the legislature intended to deprive health care workers of privacy rights "merely because they are using their biometric information for the purpose of patient treatment." (*Id*. at 6 (citing Hr'g Tr. 53:1–22, *Bruhn v. New Albertson's, Inc.*, No. 2018 CH 01737 (Ill. Cir. Ct. Cook Cnty. July 2, 2019)).) Since then, other courts have weighed in,[7] and the court now concludes that BD's interpretation lacks merit.

First, the court notes that if the Illinois legislature had intended to exclude health care workers from BIPA, there was a much more straightforward means to do so. Section 25 provides explicit carveouts for financial institutions and government contractors. *See* 740 ILCS 14/25(c) ("Nothing in this Act shall be construed to apply in any manner to a financial institution. . . ."); 740 ILCS 14/25(e) ("Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government . . . ."). Yet the legislature did not include a provision explicitly stating that BIPA shall not be construed to apply to a health care provider, much less a biometric-device vendor. Alternatively, the legislature could have excluded health care institutions from the definition of private entity, but it did not. *See* 740 ILCS 14/10 ("A private entity does not include a State or local government agency.").

Defendant is correct that another provision in Section 25 states that "[n]othing in this Act shall be construed to conflict with . . . [HIPAA]" (MTD Mem. at 11), but that provision is beside the point unless BD is a covered entity within the meaning of HIPAA. 740 ILCS 14/25(b). HIPAA

[7] *See Peaks-Smith v. St. Anthony's Hosp.*, No. 18 CH 07077 (Ill. Cir. Ct. Cook Cnty. Jan. 7, 2020) (Ex. 1 to MTD Opp'n [53-1]); *Mosby v. Ingalls Mem'l Hosp.*, No. 18 CH 05301 (Ill. Cir. Ct. Cook Cnty. Jan. 13, 2020) (Ex. 2 to MTD Opp'n [53-2]); *Winters v. Aperion Care Inc.*, No. 19-CH-6579 (Ill. Cir. Ct. Cook Cnty. Feb. 11, 2020) (Ex. 3 to MTD Opp'n [53-3]).

applies to health care plans, health care clearinghouses, and health care providers who transmit health information electronically "in connection with a transaction covered by [HIPAA]." 45 C.F.R. § 165.104. BD falls into none of these categories. Defendant responds that "BD's status under HIPAA is wholly irrelevant" because "the clause refers to HIPAA only to identify the types of information exempted from BIPA, not the entities exempted from BIPA." (MTD Reply at 8 n.5.) But if BD is not a HIPAA covered entity, then its reading of Section 10 of BIPA falls apart: BD is not "collect[ing], us[ing], or stor[ing]" biometric data "for health care treatment, payment, or operations *under [HIPAA]*." 740 ILCS 14/10 (emphasis added). The court reads the phrase "for health care treatment . . . under [HIPAA]" to mean biometric information "collected by a HIPAA covered entity for the purpose of health care treatment, payment, or operations." In short, if HIPAA does not apply to BD, then BD cannot claim protection from the HIPAA exemption. Moreover, given that HIPAA protects *patient* health information, not medical provider information, it would be odd for the legislature to exclude biometric data from BIPA protection that is not even protected under HIPAA.

Only one state court has adopted BD's preferred interpretation. *See Diaz v. Silver Cross Hosp.*, No. 2018 CH 00137 (Ill. Cir. Ct. Will Cnty. Aug. 29, 2019) ("*Diaz I*") (Ex. 1 to Def.'s Reply in Support of Mot. to Dismiss [29-1]) (finding that a health care exclusion applied but allowing plaintiff to amend her complaint); *Diaz v. Silver Cross Hosp.*, No. 2018 CH 00137 (Ill. Cir. Ct. Will Cnty. July 6, 2020) ("*Diaz II*") (Ex. 2 to MTD Reply [57-2]) (reaching the same result when ruling on a renewed motion to dismiss plaintiff's amended complaint). In *Diaz II*, the entirety of the court's statutory interpretation is contained in the following sentence: "I don't believe that BIPA covers the situation we have at [ ] hand where [defendants] are collecting the biometric information for an employee who is handing out opioids or prescriptions pharmaceuticals." (Ex. 2 to MTD Reply at 4.) However persuasive that statement may be, the facts of *Diaz* are distinguishable. The defendant in that case was a hospital, thus clearly covered by HIPAA. (*See*

Hr'g Tr. 5:20–22, *Diaz I* ("To [defendant's] knowledge, this case is a matter of first impression as to the . . . BIPA HIPAA exemption applicability *to hospitals*.") (emphasis added)).

By contrast, judges in four other state court cases have concluded that there is no such exemption for health care workers' biometric information. *See* Hr'g Tr. 38:3–16, 53:4–55:13, *Bruhn v. New Albertson's, Inc*, No. 2018 CH 01737 (Ill. Cir. Ct. Cook Cnty. July 2, 2019) (calling defendants' interpretation "a doughnut hole that I can't fathom the legislature intended"); *Peaks-Smith v. St. Anthony's Hosp.*, No. 18 CH 07077 (Ill. Cir. Ct. Cook Cnty. Jan. 7, 2020) (Ex. 1 to Opp'n to MTD [53-1] at Hr'g Tr. 26:4–27:13, 31:3–33:9 (denying motion to dismiss on the basis of the HIPAA exemption, but allowing defendant to raise the argument again after discovery); *Mosby v. Ingalls Mem'l Hosp*., No. 18 CH 05031 (Ill. Cir. Ct. Cook Cnty. Jan. 13, 2020) (Ex. 2 to Opp'n to MTD [53-2] at Hr'g Tr. 67:14–68:3) ("HIPAA, by its terms, does not protect the privacy of health care employees' biometric information. It protects patients. And if the legislature intended to exempt them entirely from [BIPA], I'd expect the legislature to do so in a more explicit and straightforward way."); *Winters v. Aperion Care Inc.*, No. 19-CH-6579 (Ill. Cir. Ct. Cook Cnty. Feb. 11, 2020) (Ex. 3 to Opp'n to MTD [53-3] at *7–8) ("[T]he plain and unambiguous language of section 14/10 applies to information collected *from a patient* and not information collected from health care workers or providers."). If Illinois appellate courts eventually weigh in and disagree with this court's interpretation, the court will grant Defendant leave to raise this argument again.[8]

E. State of Mind

Alternatively, BD contends that Plaintiff's claims should be dismissed because he failed to plead negligence, recklessness, or intent on the part of Defendant. Section 20 of the BIPA provides that plaintiffs may recover "$1,000 or actual damages, whichever is greater" for negligent violations, and "$5,000 or actual damages, whichever is greater" for reckless or intentional

[8] For example, the court is aware that the Illinois Supreme Court recently directed the First District to answer a certified question in *Mosby*, possibly on this issue. *See Mosby v. Ingalls Mem'l Hosp.*, No. 126590, 2021 WL 631765, at *1 (Ill. Jan. 27, 2021).

violations. 740 ILCS 14/20(1)–(2). Courts have recognized that "the cases have split as to whether a defendant's mental state is a pleading requirement" for plaintiffs seeking statutory damages under BIPA. *Figueroa*, 454 F. Supp. 3d at 786; *compare Namuwonge*, 418 F. Supp. 3d at 286 (dismissing plaintiff's claim for damages based on intentional and reckless conduct but concluding that the complaint alleged enough facts for damages based on negligent conduct), *with Woodward v. Dylan's Candybar LLC*, No. 19 CH 05158, slip op. at 7 (Ill. Cir. Ct. Cook Cnty. Nov. 20, 2019) (holding that plaintiff need not plead facts showing defendant's state of mind before seeking liquidated damages under BIPA).

Because BIPA was enacted in 2008, over a decade ago, several district courts have inferred that a defendant was at least negligent for failing to comply with BIPA today. *See Namuwonge*, 418 F. Supp. 3d at 286; *Figueroa*, 454 F. Supp. 3d at 786 ("Because a motion to dismiss under Rule 12(b)(6) doesn't permit piecemeal dismissals of *parts* of claims, that the complaint's factual allegations give rise to an inference of negligence is enough to withstand dismissal.") (internal quotation marks and citation omitted, emphasis in original). Some courts have gone further, concluding that a defendant's alleged failure to comply with BIPA permits an inference of recklessness or intent. *See Neals*, 419 F. Supp. 3d at 1092–93; *Marsh v. CSL Plasma, Inc.*, ___ F. Supp. 3d ___, No. 19 C 6700, 2020 WL 7027720, at *6 (N.D. Ill. Nov. 30, 2020); *Rogers v. BNSF Ry. Co.*, 2019 WL 5635180, at *5 (N.D. Ill. Oct. 31, 2019). "To be sure, discovery might very well undermine the recklessness or intent allegation, and at a trial, the shoe would be on the other foot, with the Plaintiff[ ] bearing the burden of proof." *Marsh*, 2020 WL 7027720, at *6. For now, though, the court concludes that Plaintiff has alleged enough facts to infer that Defendant's failure to comply with BIPA was negligent, reckless, or even intentional (*see, e.g.*, FAC ¶¶ 100, 108–09, 118), and rejects Defendant's argument for categorical dismissal of Plaintiff's liquidated damages claims.

II. Motion to Strike Class Allegations

Having denied Defendant's motion to dismiss, the court turns to BD's motion to strike Plaintiff's class allegations. FED. R. CIV. P. 23(c)(1)(A) provides: "At an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action." In "limited circumstances," a court may rule on class allegations at the pleading stage. *Al Haj v. Pfizer Inc.*, 338 F. Supp. 3d 741, 757 (N.D. Ill. 2018); *see Kasalo v. Harris & Harris, Ltd.*, 656 F.3d 557, 563 (7th Cir. 2011) ("[A court] need not delay a ruling on certification if it thinks that additional discovery would not be useful in resolving the class determination."). Striking class allegations before discovery is appropriate if the class allegations are "facially and inherently deficient." *Figueroa*, 454 F. Supp. 3d at 787 (quoting *Buonomo v. Optimum Outcomes, Inc.*, 301 F.R.D. 292, 295 (N.D. Ill. 2014)). But "[i]f . . . the dispute concerning class certification is factual in nature and discovery is needed to determine whether a class should be certified, a motion to strike the class allegations at the pleading stage is premature." *Figueroa*, 454 F. Supp. 3d at 787 (quoting *Buonomo*, 301 F.R.D. at 295).

So it is in this case. BD has argued that Plaintiff cannot satisfy Rule 23(b)(3)'s superiority and predominance requirements for class actions seeking damages. (Def.'s Mem. in Support of Mot. to Strike [46] (hereinafter "Mot. to Strike Mem.") at 3–11). Additionally, BD contends that Mr. Heard's involvement in other BIPA class actions renders him an inadequate class representative in this case. (*Id*. at 12–13.) As explained below, the court concludes these arguments are premature. To the extent that the proposed class is overbroad as currently defined, the appropriate response is to narrow the class definition rather than denying class certification entirely at the pleading stage. *See Messner v. Northshore Univ. HealthSystem,* 669 F.3d 802, 825–26 (7th Cir. 2012) (collecting cases in which courts revised class definition rather than denying certification). Accordingly, the court denies the motion to strike class allegations without prejudice.

A. Superiority

A class satisfies the superiority requirement if "a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." FED. R. CIV. P. 23(b)(3). Rule 23 further directs courts to consider the following factors: "(A) the class members' interests in individually controlling the prosecution or defense of separate actions; (B) the extent and nature of any litigation concerning the controversy already begun by or against class members; (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (D) the likely difficulties in managing a class action." *Id*.

1. Manageability

Defendant argues that the putative class will be unmanageable for a host of reasons. As currently defined, the class would include: "All users in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by Defendant during the applicable statutory period." (FAC ¶ 83.) According to the FAC itself, Pyxis users work for a variety of businesses in the health care industry, including hospitals, research laboratories, and pharmacies. (*Id*. ¶ 1.) BD insists that it has no direct relationship with the employees of its customers, so third-party discovery would be necessary to identify all Pyxis users. (Mot. to Strike Mem. at 4.) Third-party discovery would also be necessary to determine, among other things: whether each BD customer executed BIPA-compliant releases or consent forms with customers' employees, which might shield BD from liability; whether some Pyxis users were subject to collective bargaining agreements; and whether customers performed government contract work. (*Id*. at 5.) Furthermore, some members of the proposed class may already be members of Mr. Heard's BIPA suits against hospitals. *See, e.g.*, *Heard v. Weiss Mem'l Hosp.*, No. 19 CH 06763 (Cir. Ct. Ill. Cook Cnty.) Finally, BD insists that the court will need to monitor all other BIPA class actions that name or potentially implicate it. (Mot. to Strike Mem. at 5.)

Although the court agrees that the proposed class would be challenging to manage, those challenges are not so insurmountable as to justify striking the class allegations at the pleading stage. *See Mullins v. Direct Digital, LLC*, 795 F.3d 654, 664 (7th Cir. 2015) (noting that "refusing to certify on manageability grounds alone should be the last resort"). Proceeding as a class action in this case could still be a superior means for litigating many relatively small claims. *See Suchanek v. Sturm Foods, Inc.*, 764 F.3d 750, 759 (7th Cir. 2014) ("The policy at the very core of the class action mechanism is to overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action prosecuting his or her rights.") (citation omitted). If some or all of the issues BD has identified arise after discovery, BD can raise them again in connection with briefing a motion for class certification. And Plaintiff may seek leave to certify a different class or subclasses. *See* FED. R. CIV. P. 23(c)(5), (d)(1)(D).

2. Ascertainability

Next, BD argues that the class definition fails Rule 23's "ascertainability" requirement. Defendant characterizes this requirement as both practical and implicit. Practically, it would be "impossible" to identify which of BD's customers' employees had enrolled on Pyxis devices because BD does not possess information about its customers' internal operations. (Mot. to Strike Mem. at 6.). The court agrees with Plaintiff, however, that this can be sorted out in discovery. BD surely knows who its own customers are, and "nothing on the face of Plaintiff's FAC suggests that BD does not know whose biometric data it collected and possesses." (Opp'n to Mot. to Strike [55] at 18.) Moreover, the Seventh Circuit has rejected the "heightened ascertainability requirement"—adopted by some courts—that plaintiffs must prove "there is a reliable and administratively feasible way to identify all who fall within the class definition." *Mullins*, 795 F.3d at 657 (internal quotation marks omitted). Instead, the Seventh Circuit has instructed lower courts to focus on the "established meaning" of ascertainability, which asks whether the class can "be defined clearly and based on objective criteria." *Id*. at 659.

Turning to Rule 23's implicit requirement of ascertainability, BD insists that the class cannot be defined clearly by objective criteria because membership is defined in terms of success on the merits. (*Id*. at 6 n.6 (citing *Mullins*, 795 F.3d at 657).) Again, the putative class includes "[a]ll users in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed" by BD. (FAC ¶ 83.) BD contends that Plaintiff has proposed a "fail-safe class," and courts have routinely recognized that such classes are not properly defined. *See Mullins*, 795 F.3d at 660 (collecting cases). Class membership should not depend on the liability of the defendant; otherwise, members of classes that fail on the merits would be free to try again because, "by virtue of losing, [they are] defined out of the class and [ ] therefore not bound by the judgment." *Id*. (quoting *Messner,* 669 F.3d at 825).

The court disagrees that the putative class is a fail-safe class. The proposed definition is not "all users in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by BD *in violation of BIPA*." Such a definition would clearly tie class membership to BD's liability. Furthermore, BIPA does not prohibit collecting, capturing, receiving, or otherwise obtaining biometric data in all circumstances; rather, it imposes conditions on private entities who do so—namely, obtaining informed consent. *See* 740 ILCS 14/15(b). In short, whether BD collected or otherwise obtained users' fingerprints is a threshold question that will need to be resolved before the ultimate question of liability.

Finally, BD suggests that this class is duplicative of other class actions, such as Mr. Heard's employer-specific suits against hospitals that use BD's Pyxis devices. The court agrees with Plaintiff that BD's argument would improperly expand the so-called duplicativeness doctrine. In *Copello v. Boehringer Ingelheim Pharm. Inc.*, a district court dismissed a putative class action where a certified collective action in another suit was raising the same claims against the same defendant, and a named plaintiff had already opted into the certified collective action. 812 F. Supp. 2d 886, 889–90 (N.D. Ill. 2011). By contrast, this suit focuses on BD's course of conduct,

not the hospitals. Although BD is a co-defendant in at least one other BIPA class action, *see Mosby v. Ingalls Mem'l Hosp*., 18 CH 05031 (Cir. Ct. Ill. Cook Cnty.), the court does not yet have information to determine whether that class is duplicative in the sense that the *Copello* court meant. This court will of course revisit the issue if the class in *Mosby* is certified and BD is still a defendant in that suit.

B. Predominance

A class satisfies the predominance requirement if "questions of law or fact common to class members predominate over any questions affecting only individual members." FED. R. CIV. P. 23(b)(3). The predominance inquiry "tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation," *Amchem Prods. Inc. v. Windsor*, 521 U.S. 591, 623 (1997), "but it scarcely demands commonality as to all questions." *Comcast Corp. v. Behrend*, 569 U.S. 27, 41 (2013) (Ginsburg, J, dissenting). "In particular, when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate." *Comcast*, 569 U.S. at 41; *see also Chi. Teachers Union, Local No. 1. v. Bd. of Educ. of City of Chi.*, 797 F.3d 426, 443–44 (7th Cir. 2015) (applying Justice Ginsburg's characterization of the predominance inquiry). Predominance fails when "affirmative defenses will require a person-by-person evaluation of conduct to determine whether [a defense] precludes individual recovery." *Figueroa*, 454 F. Supp. 3d at 789 (citations omitted). "To justify striking class allegations on predominance grounds at the pleadings stage, a defendant must 'present . . . specific evidence—as opposed to mere speculation—that [a] purportedly individualized issue predominates over common issues." *Id*. (quoting *Buonomo*, 301 F.R.D. at 298).

BD argues that individualized questions of law and fact predominate over common questions. According to BD, factual questions requiring individualized proof include: "(i) where, when, and for which employees each employer used BD devices; (ii) whether the employer's

compliance with BIPA extends to BD; (iii) whether each employee knew and understood that the devices were scanning their fingers; (iv) whether each employer allowed some or all of its employees to opt for other authentication methods . . . ; (v) when each employer used BD devices, and whether other devices were also in use; and (vi) where each employer stored employee data, for how long, and with what safeguards." (Mot. to Strike Mem. at 8.) The *Figueroa* court considered a materially identical list of factual questions and rejected the defendant's attempt to strike class allegations at the pleading stage. *See Figueroa*, 454 F. Supp. 3d at 789–90. This court agrees with the *Figueroa* court that many of these questions are simply not pertinent to Defendant's liability. *Id*. at 790 (noting that "whether some employees knew that their employers' timekeeping devices were scanning their fingerprints, or whether some employees voluntarily opted to use [defendant's] equipment rather than some other timekeeping method, appears at this point to have no bearing on whether [defendant] informed such employees that *it* was collecting their biometric data or whether it obtained their consent"). Without "specific evidence—as opposed to mere speculation—that [a] purportedly individualized issue predominates over common issues," the court cannot conclude that individualized factual questions predominate. *Buonomo*, 301 F.R.D. at 298.

The individualized legal questions that BD identifies are similarly speculative and do not defeat predominance at this time. First, BD argues that federal labor law will preempt many putative class members' claims. Pointing to *Miller v. Sw. Airlines Co.*, 926 F.3d 898 (7th Cir. 2019), BD suggests that this court will need to individually determine whether users' collective bargaining agreements impact BD's liability. In *Miller*, the Seventh Circuit held that the Railway Labor Act required that BIPA claims by unionized employees against their employers must be resolved by an adjustment board, and therefore the federal court lacked jurisdiction. *Miller*, 926 F.3d at 903–04. Subsequent district court opinions have extended *Miller* to employment contexts governed by the Labor Management Relations Act. *See, e.g.*, *Fox v. Dakkota Integrated Sys.*

LLC, No. 19-cv-2872, 2020 WL 8409682, at *3–4 (N.D. Ill. May 26, 2020), *overruled on other grounds*, 980 F.3d 1146 (7th Cir. 2020). But as the *Figueroa* court observed, "it is speculative at this stage for [defendant] to suggest that claims involving a non-employer equipment vendor like [defendant] will turn on interpreting a collective bargaining agreement to which it was not a party." *Figueroa*, 454 F. Supp. 3d at 789–90.

BD's second argument, that individual arbitration agreements may preempt putative class members' claims, is also premature. For support, BD points to an order in a state court case dismissing employees' claims against both Southwest Airlines and its technology provider, Kronos, purportedly because Southwest's alternative dispute resolution program compelled individual arbitration. (*See* Order of Jan. 24, 2019, *Battles v. Sw. Airlines Co.*, No. 18-CH-09376, Ex. C to Mot to Strike [46-3] ¶ 1). But the order does not specify that Southwest's arbitration agreement is what moved the court to dismiss claims against the third-party vendor at all, and those claims were dismissed without prejudice. (*See id.* ¶ 3.) The other cases that BD cites are easily distinguishable. *See Miracle-Pond v. Shutterfly, Inc.*, No. 19 C 4722, 2020 WL 2513099, at *6–8 (N.D. Ill. May 15, 2020) (granting motion to compel arbitration where customer consented to arbitration in clickwrap agreement); *Crooms v. Sw. Airlines Co.*, 459 F. Supp. 3d 1041, 1053–54 (N.D. Ill. 2020) (granting motion to compel arbitration in employees' BIPA suit against their employer). Here, there is simply no evidence at this time that users of the Pyxis device signed arbitration agreements with their employers that preempt BIPA claims, much less that those agreements extend to third-party vendors like BD.

Next, BD suggests that some users or their employers may perform government contract work, and the court will need to individually determine whether BIPA's government contractor exception extends to BD. (Mot. to Strike Mem. at 11.) The plain language of BIPA's government contractor exception makes clear that it applies to contractors, subcontractors, and agents of state or local governments "when working for that State agency or local unit of government." 740 ILCS

14/25(e). It is not at all clear, however, that the exception covers biometric device vendors whose customers work as government contractors. BD has not identified any case suggesting that the exemption should be read so broadly. Nor has it supplied evidence that any of its customers or their employees work as government contractors within the meaning of BIPA. At this stage, prior to discovery, BD's argument is purely speculative. *See Figueroa*, 454 F. Supp. 3d at 791 (reaching same conclusion).

Finally, BD suggests that abstention issues may arise due to the existence of concurrent state court actions. (Mot. to Strike Mem. at 12 (citing *Colorado River Water Conservation Dist. v. United States*, 424 U.S. 800, 817; *Tyrer v. City of S. Beloit*, 456 F. 3d 744, 754 (7th Cir. 2006)).) Defendant has identified only one BIPA class action in which BD is currently a named defendant. *See Mosby v. Ingalls Mem'l Hosp.*, No. 18 CH 05031 (Ill. Cir. Ct. Cook Cnty.). As Plaintiff points out, no party has requested that this court abstain pending the resolution of a state court case or cases. (Opp'n to Mot. to Strike at 14.) And even if a party did, the court fails to see how the abstention analysis would vary significantly among individual class members. *See Figueroa*, 454 F. Supp. 3d at 791 (concluding that defendant's "cursory invocations of *Colorado River* abstention . . . [do not] justify striking class allegations at this stage"). Accordingly, the court denies BD's motion to strike the class allegations on the basis of predominance.

C. Adequacy

Under Rule 23(a), named plaintiffs in a class action must "fairly and adequately protect the interests of the class." FED. R. CIV. P. 23(a)(4). "A named plaintiff must be a member of the putative class and have the same interest and injury as other members." *Beaton v. SpeedyPC Software*, 907 F.3d 1018, 1027 (7th Cir. 2018) (citation omitted). But a class representative may be inadequate if he has a conflict of interest with unnamed members of the class. *See Randall v. Rolls-Royce Corp.*, 637 F.3d 818, 824 (7th Cir. 2011).

BD argues that Mr. Heard is an inadequate class representative because he has filed employer-specific BIPA lawsuits that overlap with the proposed class in this suit, potentially creating conflicts of interest. Specifically, Mr. Heard may have incentives to sell short the class members in this suit, who may be excluded later due to labor law preemption or arbitration agreements, in favor of his employer-specific suits. Or, he might reach a settlement with BD in another case, leaving this class without a representative. (Mot. to Strike Mem. at 12–13.) These concerns, too, appear to be premature; if such problems materialize, the court will be able to address them at the class certification stage. *See Figueroa*, 454 F. Supp. 3d at 792 (reaching the same conclusion in denying a motion to strike class allegations for inadequacy at the pleading stage).

CONCLUSION

For the foregoing reasons, Defendant's motion to dismiss [43] is denied. Defendant's motion to strike class allegations [45] is denied without prejudice; BD may raise its Rule 23 arguments again after discovery. BD shall answer the FAC by April 15, 2021.

ENTER:

Dated: March 9, 2021

REBECCA R. PALLMEYER
United States District Judge